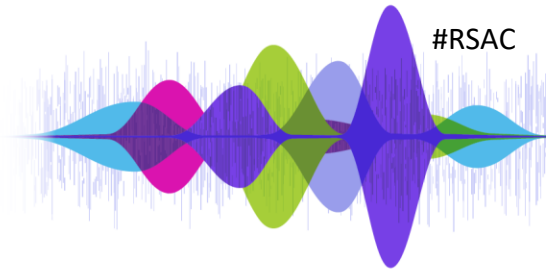
RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: GRC-R06

# One Exception Platform: Streamlining Security Exception Oversight



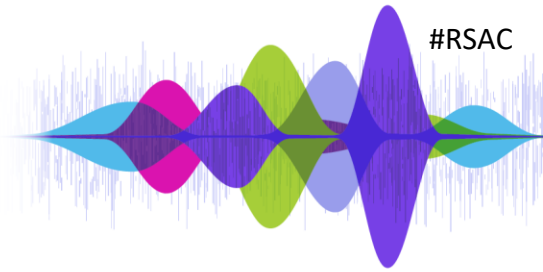
# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The facts, opinions, and data points discussed in this presentation do not represent Humana's official position or viewpoint. All information provided is based on publicly available research external to the organization. This presentation is intended for informational purposes only and should not be interpreted as an endorsement or policy statement.



# Executive Summary

## Overview:

This presentation focuses on **security exception management** and its impact on risk mitigation, compliance, and operational efficiency. It highlights **industry trends, challenges, and a technical solution** designed to streamline exception handling while ensuring governance and security oversight.

## Key Insights:

- **Risk Landscape & Industry Trends:** Misconfigurations are a leading cause of security breaches.
- **Challenges in Exception Management:** Gaps in tracking, scope creep, and manual overhead create inefficiencies and security risks.
- **Proposed Solution:** A **centralized exception management platform** that integrates with GRC tools, ensures **real-time monitoring**, and enforces standardized policies.
- **Operational Efficiency:** The solution accelerates application deployment by **70%**, reducing time from development to production.
- **Governance & Compliance:** Structured workflows, automated tracking, and reporting enhance security posture and regulatory compliance.

## Call to Action:

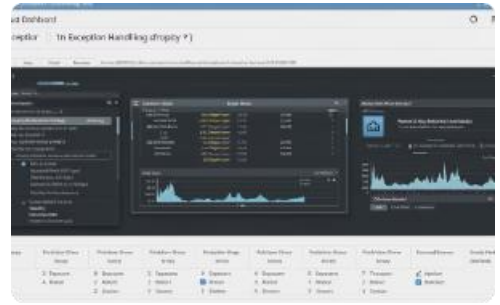
Organizations should adopt a **strategic, automated approach to exception management** to improve security, efficiency, and compliance. The implementation roadmap includes **gap analysis, proof of concept (POC), production deployment, and continuous monitoring.**

# Agenda

**1** Risk Landscape & Industry Trends - Overview of current security challenges and emerging threats

**2** Exception Management - Gaps & Business Impact - Identifying critical weaknesses and their organizational effects

**3** One Exception Platform: Architecture & Implementation - Technical overview of the proposed consolidated solution



**4** Demo: Exception Handling in Action - Practical application of the platform's capabilities

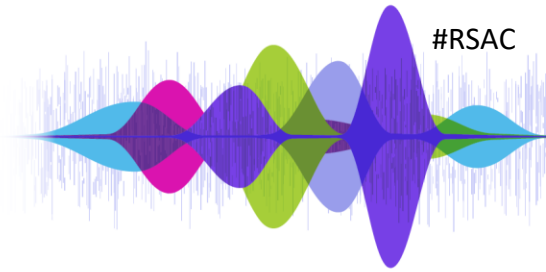
**5** Case Study - Examining real-world scenarios and solution approaches

**6** Applying Lessons Learned - Practical steps for successful implementation

**7** Q&A
Interactive discussion and addressing questions

# Industry Trends : Exception Management Failures





**78%**

### Security Incidents

Percentage of breaches linked to poorly managed security exceptions

*Source: Cybersecurity Ventures, 2023*

**63%**

### Compliance Violations

Organizations experiencing audit failures due to undocumented exceptions

*Source: Ponemon Institute, 2023*

**49%**

### Increased Risk

Higher likelihood of data exposure from exception sprawl

*Source: IBM Security Report, 2022*

### Exception Lifecycle Issues

82% of security exceptions lack proper expiration dates or review cycles, creating permanent vulnerabilities

*Source: Forrester Research, 2023*

### Documentation Gaps

71% of organizations cannot trace the business justification for existing exceptions during security audits

*Source: SANS Institute Survey, 2022*

### Governance Breakdown

Without centralized tracking, 64% of companies experience "exception creep" as temporary workarounds become permanent

*Source: IDC Security Survey, 2023*

# Industry Trends : Exception Management Failures by Industry

## Healthcare

**76%** of healthcare breaches involved unmanaged security exceptions

- Patient data exposed through expired firewall exceptions
- 42% increase in ransomware attacks targeting exception gaps

*Source: HHS Breach Portal, 2023*

## Financial Services

**68%** of financial institutions experienced incidents from **poor exception governance**

- Undocumented API exceptions led to $4.2M average breach cost
- Exception documentation gaps cited in 57% of regulatory findings

*Source: FINRA Cybersecurity Report, 2023*

## Technology/SaaS

**82%** of cloud **security incidents** linked to exception management failures

- Temporary cloud infrastructure exceptions becoming permanent
- Multi-cloud environments averaging 3,400+ untracked exceptions

*Source: CSO Cloud Security Report, 2023*

## Retail/E-commerce

**59%** of retail breaches involved unmanaged PCI compliance exceptions

- Payment processing exceptions led to credential harvesting
- Average cost per compromised record: $180

*Source: Verizon DBIR, 2023*

## Manufacturing

**73%** of OT/IT security incidents tied to exception management failures

- Legacy systems with permanent security exceptions
- Lack of exception review processes in 82% of affected organizations

*Source: NIST Manufacturing Profile, 2023*

## Public Sector

**64%** of government agencies unable to track security exceptions effectively

- Nation-state actors exploiting known exception gaps
- Average remediation time: 280 days vs. industry average of 97 days

*Source: CISA Threat Assessment, 2023*

Humana

Research indicates organizations with mature exception management processes reduce their breach likelihood by 72% compared to organizations with ad-hoc approaches. *(Gartner Security & Risk Management Report, 2023)*

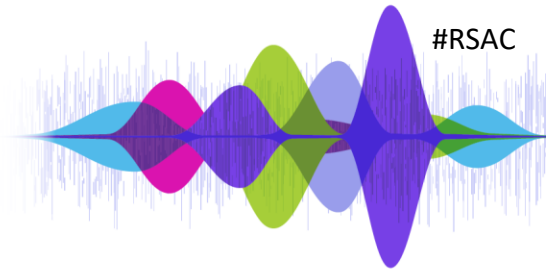
RSAC 2025 Conference

# Exception Management

## Process Overview & Gaps

Many Voices.
**One Community.**

# Exception Management: Process Overview



1

### Request Exception

Stakeholder initiates the process by submitting a formal exception request with justification.

2

### Risk Review

Security team conducts comprehensive business impact and architectural assessment to identify potential vulnerabilities.

3

### Approval

Secure authorization from request owner and leadership to ensure alignment with acceptable risk tolerance.

4

### Update GRC Tool

Systematically document and track all approved exceptions within the centralized GRC platform.

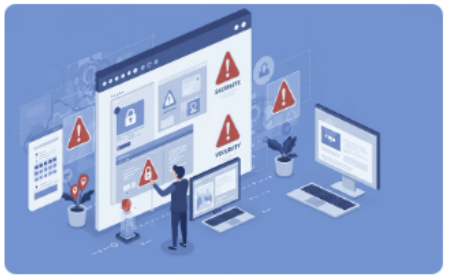
5

### Implement Exception

Deploy appropriate compensating controls to properly implement and monitor the approved exceptions.

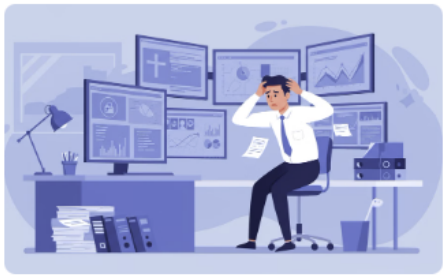
# Exception Management: Gaps

**Key challenges organizations face when managing security exceptions**



## Configuration Gaps

- Drift in configuration gaps leading to security vulnerabilities
- Untracked changes causing compliance violations
- Inconsistent application of security policies across environments
- Lack of visibility into configuration exception dependencies



## Manual Overhead

- Manual overhead for reconciling exceptions across systems
- Time-consuming approval processes leading to shadow IT
- Inefficient documentation practices causing knowledge gaps
- Resource-intensive auditing procedures with limited effectiveness

## Scope Issues

- Exceptions applied for limited time still active after expiration
- Scope of the exception approved differs from what's applied
- Lack of contextual understanding when approving exceptions
- Insufficient risk assessment during exception approval process

## Governance Challenges

- Unclear ownership of exception management processes
- Inadequate controls for exception reviews and renewals
- Fragmented tools and processes across business units
- Limited metrics for measuring exception management effectiveness

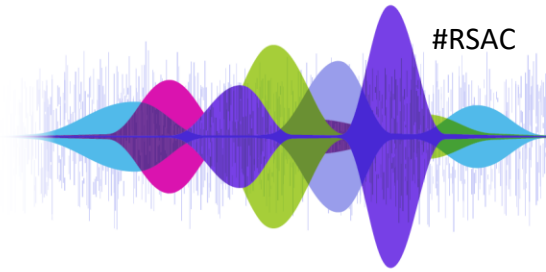
RSAC 2025 Conference

# One Exception Platform

## Architecture & Implementation

Many Voices.
**One Community.**

# Exception Management: Process Overview With Technical Platform



1

### Request Exception

Requestor submits an exception request.

2

### Risk Review

Conduct business and architectural review for potential risks.

3

### Approval

Obtain approval from request owner and leadership to align with risks.

4

### Update GRC Tool

Record the exceptions in the GRC tool.

5

### Deploy Exception

Utilize centralized technical exception platform.

6

### Reporting and Monitoring

Provides visibility and tracks changes, risk scope.

# Exception Management: Platform Differentiation



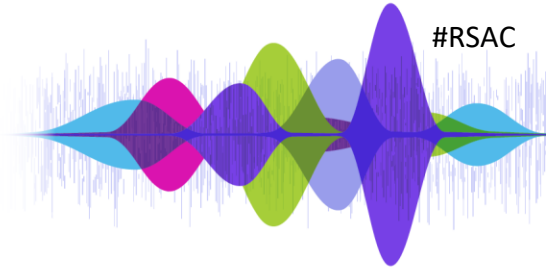
**Regular** – Manual Process, Process Overhead, Errors

1. **Request Exception**
   Stakeholder initiates the process by submitting a formal exception request with justification.
2. **Risk Review**
   Security team conducts comprehensive business impact and architectural assessment to identify potential vulnerabilities.
3. **Approval**
   Secure authorization from request owner and leadership to ensure alignment with acceptable risk tolerance.
4. **Update GRC Tool**
   Systematically document and track all approved exceptions within the centralized GRC platform.
5. **Implement Exception**
   Deploy appropriate compensating controls to properly implement and monitor the approved exceptions.

**Automated Platform** – Automated Monitoring and Deployment

1. **Request Exception**
   Requestor submits an exception request.
2. **Risk Review**
   Conduct business and architectural review for potential risks.
3. **Approval**
   Obtain approval from request owner and leadership to align with risks.
4. **Update GRC Tool**
   Record the exceptions in the GRC tool.
5. **Deploy Exception**
   Utilize centralized technical exception platform.
6. **Reporting and Monitoring**
   Provides visibility and tracks changes, risk scope.

# Exception Management: Automated Platform Considerations



### Universal Platform Integration

Leverages robust API and CLI frameworks for frictionless deployment across all environments.

### Future-Proof Architecture

Flexibly adapts and scales as your security infrastructure evolves and expands.

### Comprehensive Visibility

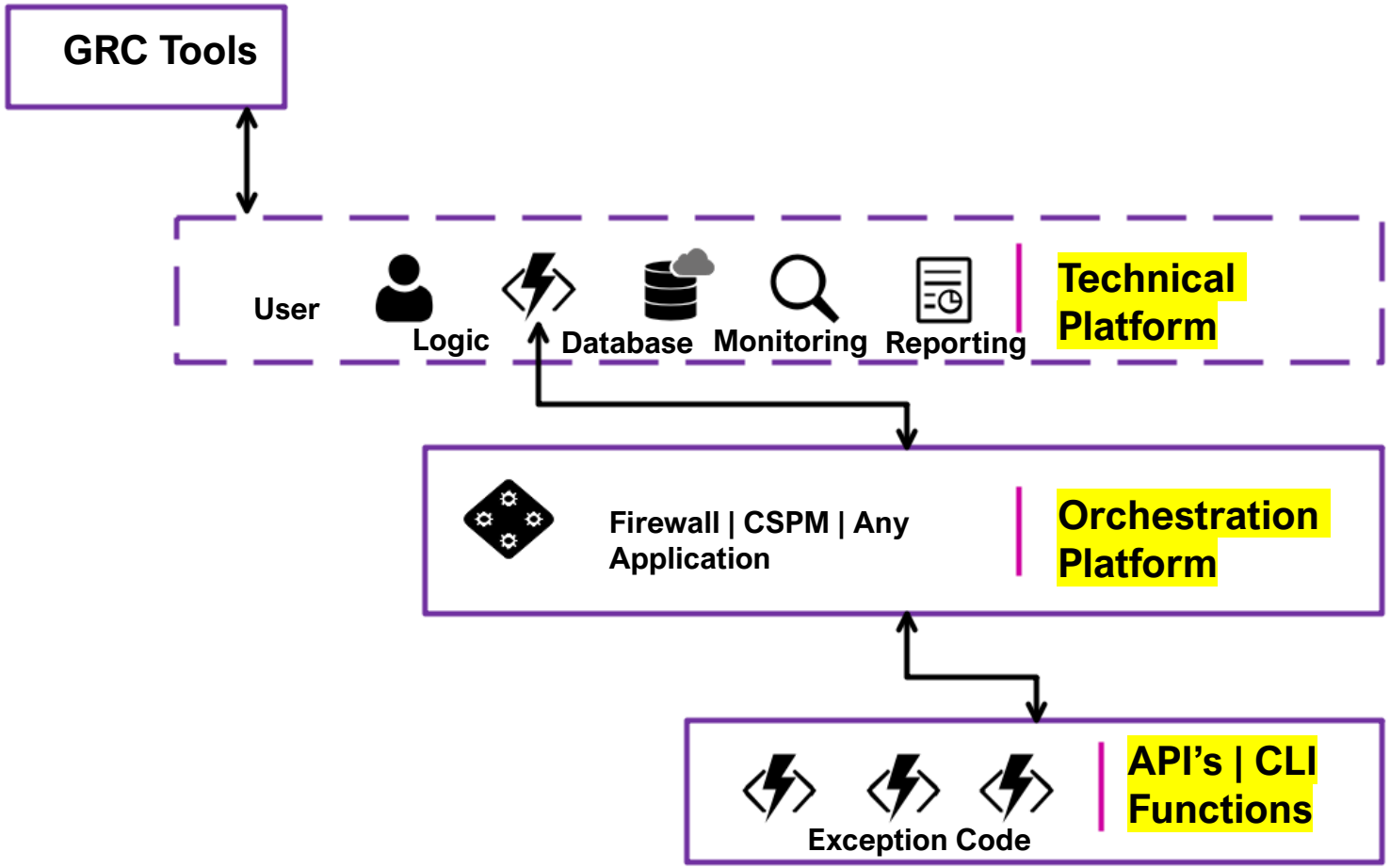
Ensures continuous monitoring with detailed analytics and tracking across all security touchpoints.

### Embedded Governance

Seamlessly integrates real-time compliance and risk management into operational workflows.

# Exception Management: Platform Architecture





RSAC 2025 Conference

# Platform Demo

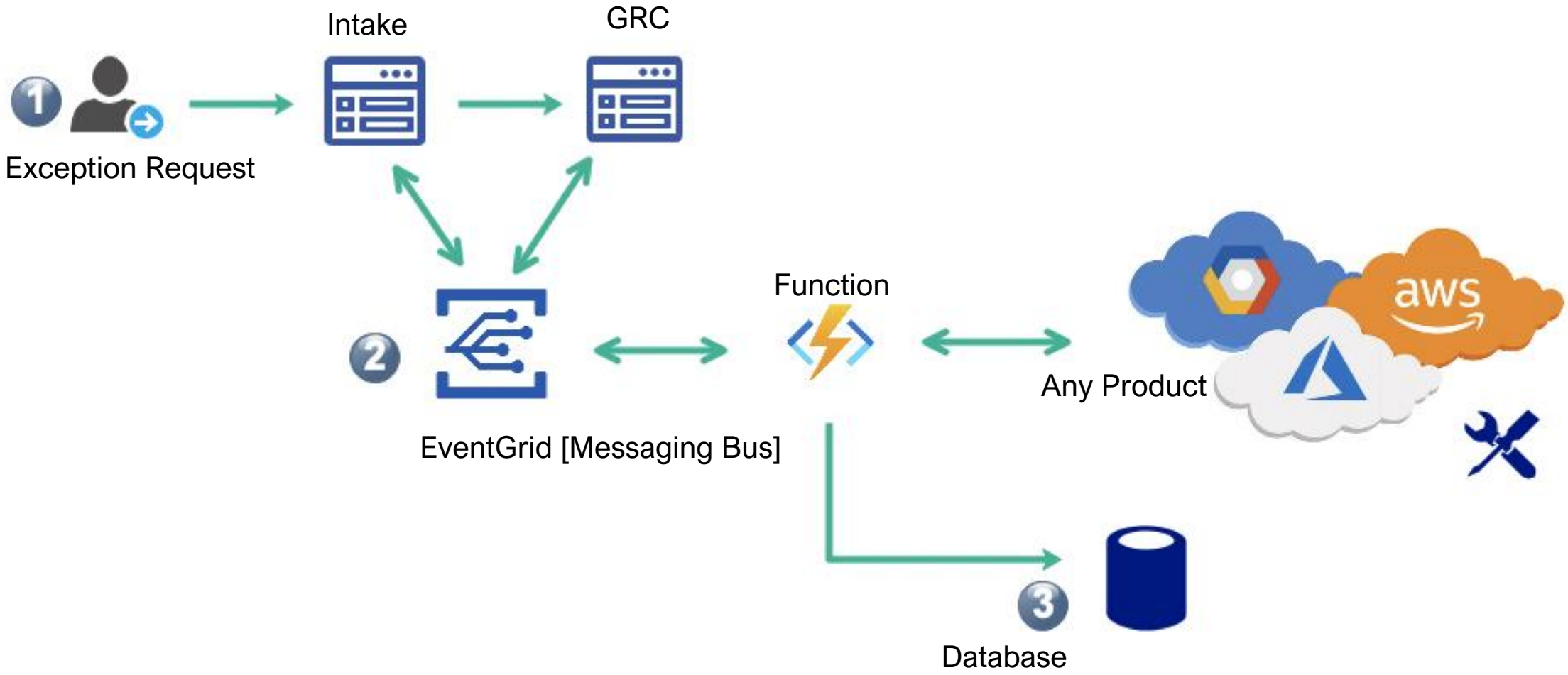
## Exception Management In Action

Many Voices.
**One Community.**

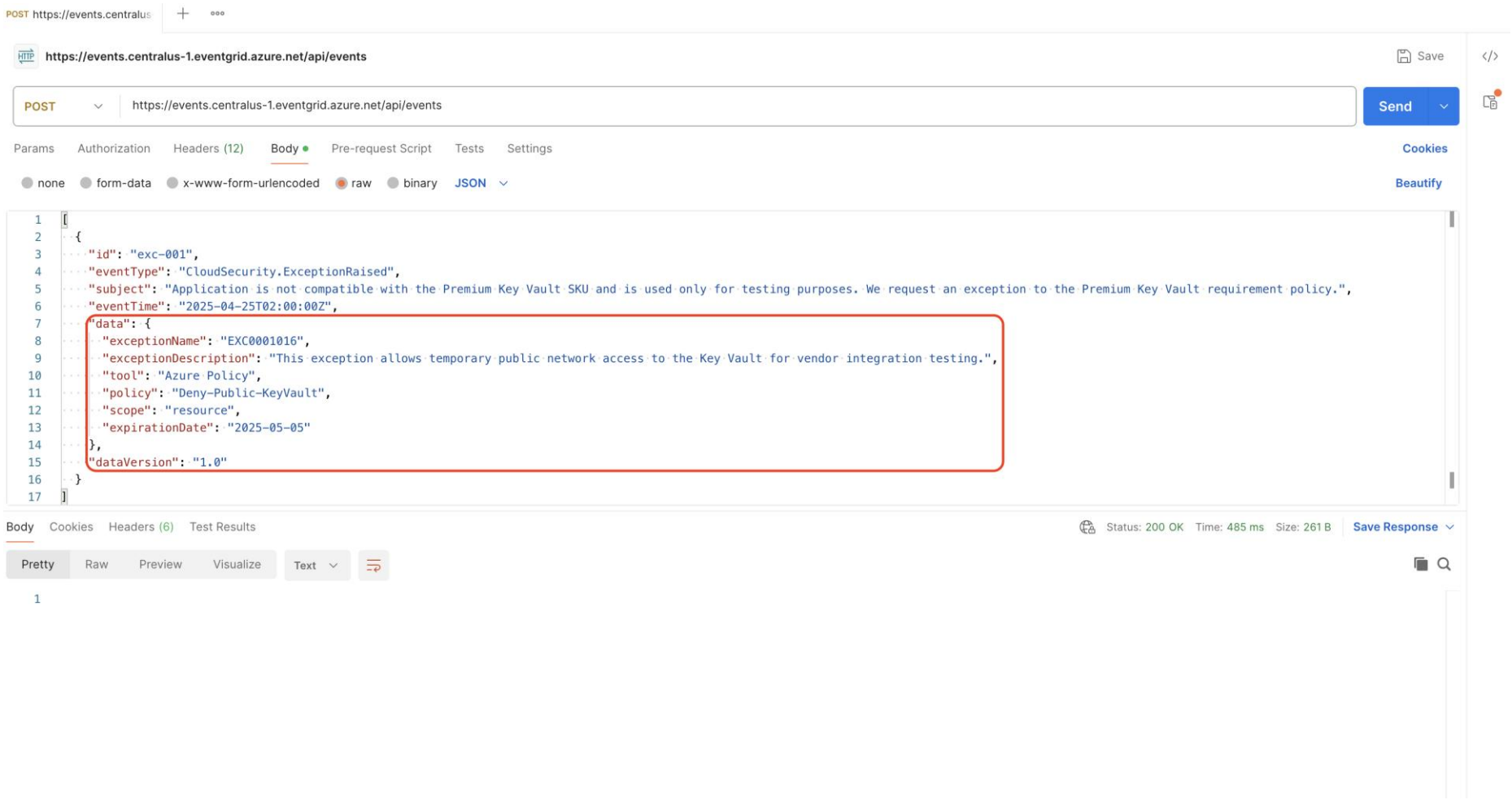
# Demo

- Exception Platform – Eramba (Open Source GRC)
- Exception Approval Workflow
- How to Integrate with technical Platform (Database and Scripts to apply the exception)
- Monitoring and Reporting
- For Demo we will apply exception in Azure Cloud via GRC tool and go though the process. It should be same for any other tool.

# Demo - Components



# Demo – Sample Event



# Demo

Intake
GRC
Request for Exception
Event Grid [Messaging Bus]
Function
Any
Text
Database [Store Results]

RSAC 2025 Conference

# Case Study

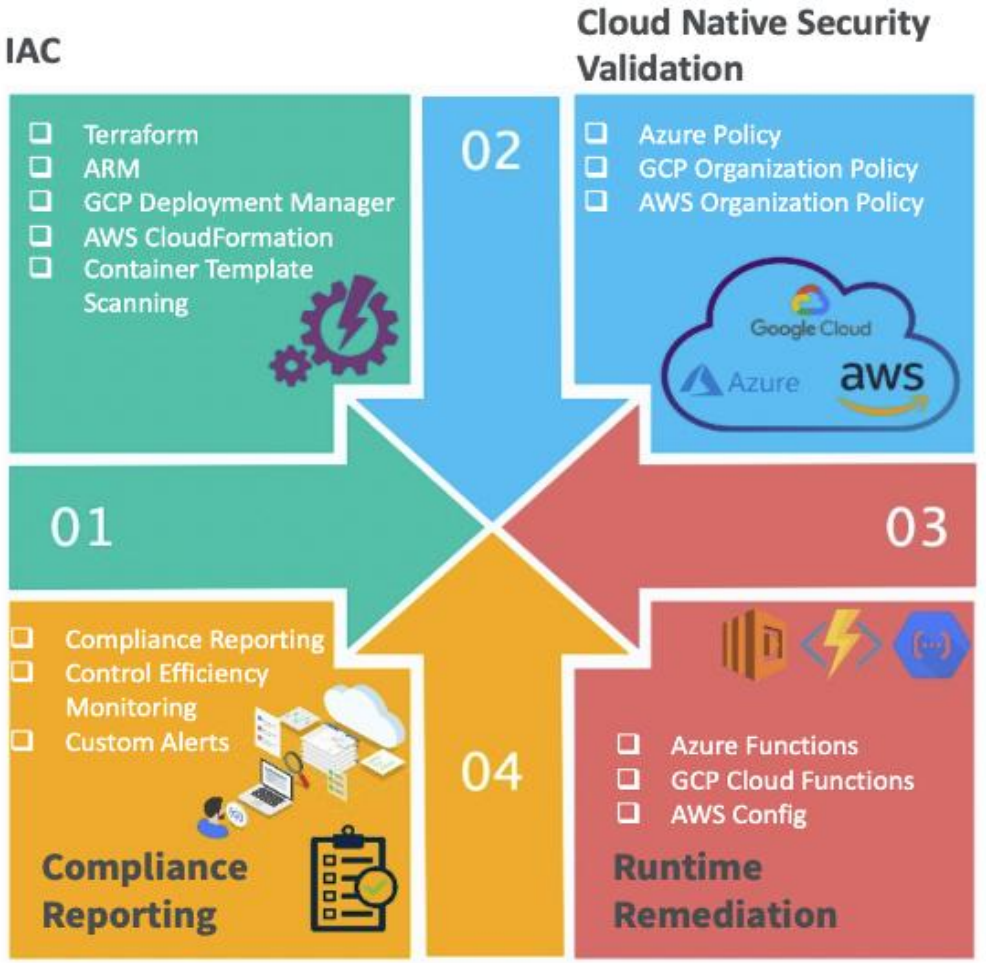
## Exception Management In Cloud

Many Voices.
**One Community.**

# Cloud Security Management

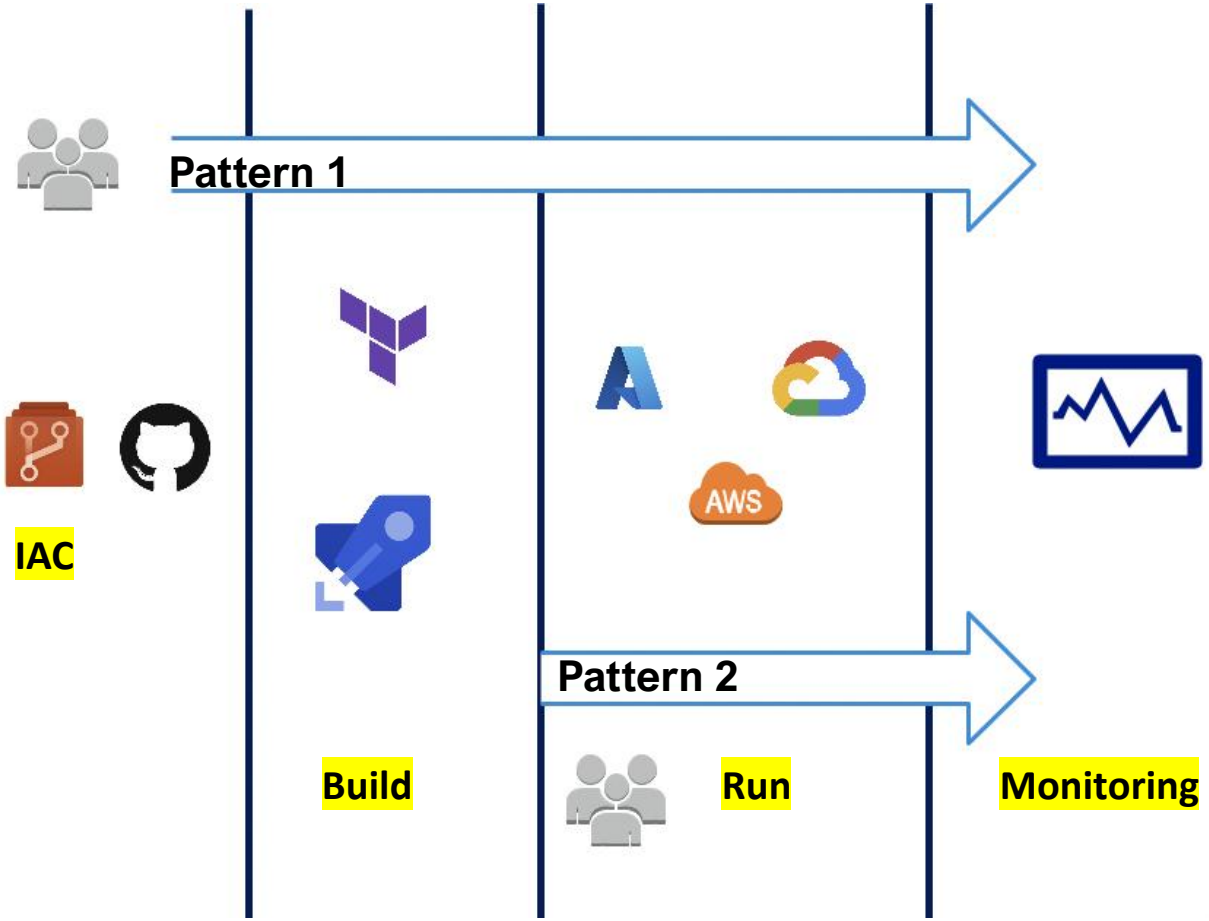
## Foundational Pillars

- IAC - Infrastructure as code scanning
- Cloud Native Security Validation
- Runtime Remediation
- Compliance Reporting



# Exceptions Management
## Use Case

- **Pattern 1:** Apply and monitor exceptions consistently across all tools to ensure successful deployment.
- **Pattern 2:** Align exceptions with the deployment process to prevent failures.
- **Crucial Part in Monitoring Risk**: Effective reporting and tracking are crucial for managing system risks.



RSAC 2025 Conference

# Business Driver

**Security exceptions, when managed strategically, can drive business growth without compromising resilience.**

# Exception Management: Business Value



### Efficient Risk Management

Transform enterprise security through strategic application assessment and prioritized risk handling.

### Residual Risk Tracking

Deliver actionable insights through continuous monitoring of residual risks, enabling proactive mitigation throughout the application lifecycle.

### Clear Exception Mapping

Provide comprehensive visibility by creating transparent relationships between exceptions and critical application components.

### Operational Efficiency

Drive **70%** faster application deployment cycles while maintaining security integrity, dramatically reducing time-to-market.

RSAC 2025 Conference

# Applying Learning

## Incorporating Exception Platform

Many Voices.
**One Community.**

# Exception Management: Technical Platform Where could you apply?

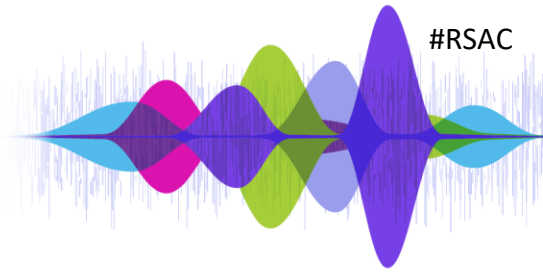


**Required:** Any application that supports API /SDK Integration

**USE CASES – On Premise / Hybrid- Public – Community / Cloud**

- Network Security Infrastructure (Firewalls, IDS/IPS, Web Application Firewalls)
- Data Protection Systems (DLP, Encryption, Access Controls)
- Cloud Security Posture Management (CSPM) Tools
- Identity and Access Management (IAM) Platforms
- Compliance Monitoring and Reporting Systems
- DevSecOps Pipelines and CI/CD Security Controls
- Vulnerability Management Systems and Scanners
- Container and Kubernetes Security Platforms
- API Security Gateways and Management Tools
- Any security control or technical infrastructure requiring configuration-based exception management

# Exception Management: Technical Platform How to Apply?




## Required: GRC Platform, Database, Scrips

**Few opensource choices for implementation**

### GRC Platforms: Opensource Implementations

- **Eramba**

### Databases

- **SQL/ NO SQL**

### Dashboards

- **ELK Stack or any other tool**

### Programming

- **Python, JS or anything of your choice**

# Exception Management: Technical Platform Implementation Timeline

**Month 1: Form Specialized Working Group**

- Assemble cross-functional team from Security, IT, Compliance and Business
- Select target security control for initial implementation
- Define scope and success metrics

**Months 1-3: Conduct Gap Analysis**

- Audit existing processes to identify visibility gaps
- Document workflows for automation opportunities
- Build POC with clear exception mapping

**Month 3-5: Present Results**

- Demonstrate cost-benefit analysis and efficiency gains
- Showcase residual risk tracking capabilities
- Secure approval for full implementation

**Month 5-6: Enterprise Deployment**

- Integrate with existing GRC processes and infrastructure
- Implement role-based access for approval workflows
- Configure time-bound exceptions with expiration alerts
- Train teams on standardized documentation procedures

**Month 6+: Continuous Monitoring**

- Deploy real-time exception dashboards for leadership
- Establish quarterly review cycles for active exceptions
- Create automated risk reports for compliance
- Expand to additional security control domains

RSAC 2025 Conference

# Questions

RSAC™ 2025 Conference

Many Voices.
**One Community.**

**Feel free to reach out with any questions**

**or for further discussions.**

**Let's connect on LinkedIn: /santosh-bompally-048758b4/**

Humana®